REMARKS

This amendment is responsive to the Office Action dated November 21, 2003. Applicants have cancelled claims 8 and 19, and amended claims 1, 2, 9-11, 16, 20-25, 32, 37-42, 45-46, 51-52, 61, and 66. Claims 1-7, 9-18, 20-66 are pending upon entry of this amendment.

Claim Rejections Under 35 U.S.C. § 112

In the Office Action, the Examiner rejected claims 1 and 2 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. In addition, the Examiner objected to claim 25 due to a typographical error. Applicants have amended claims 1, 2 and 25, as well as claims 39, 40, 46, 61, and 66 for purposes of clarification and not for purposes related to patentability. Applicants submit that these claims, as amended, particularly point out and distinctly claim the subject matter, as required by 35 U.S.C. 112, second paragraph.

Claim Rejections Under 35 U.S.C. § 102

Claims 1-6, 8, 12-21, 26-33, 45-49, 51-54, 56-61 and 63-67

In the Office Action, the Examiner rejected claims 1-6, 8, 12-21, 26-33, 45-49, 51-54, 56-61 and 63-67 under 35 U.S.C. 102(b) as being anticipated by Narasimhalu et al. (US 5,412,718). Applicants respectfully traverse the rejection to the extent such rejection may be considered applicable to the amended claims. Narasimhalu et al. fails to disclose each and every feature of the claimed invention, as required by 35 U.S.C. 102(b), and provides no teaching that would have suggested the desirability of modification to include such features.

With respect to claim 1, for example, Narasimhalu fails to teach or suggest sensing whether a storage device has device-specific security information, operating a computer in a full-access mode when the storage device has the device-specific security information, and operating the computer in a restricted-access mode when the storage device does not have the device-specific security information. Applicants have amended claim 1 to clarify that in the full-access mode the computer permits both read and write access to the storage device, and that in the restricted-access mode the computer permits read access to the storage device and prevents write access to the storage device.

In contrast to these requirements, Narasimhalu describes a copy protection scheme for preventing unauthorized copying of distributed software or other information. More specifically, Narasimhalu describes a copy protection scheme in which format non-uniformities of the distribution medium, e.g., a magnetic or optical disk, are used to control installation of (or read access to) the distributed software or other information on the medium.[1]

With respect to the requirement of operating the computer in a full-access mode, the Examiner stated that Narasimhalu discloses that non-uniformities are detected with a non-uniformities detection program (NDP), and that a decryption key enables the information consumer to decrypt the encrypted information. Consequently, it is clear that the copy protection scheme of Narasimhalu is simply for controlling installation of the distributed software by permitting the software to be read and installed based on a correct match of the media-specific non-uniformities.

In contrast to the requirements of claim 1, Narasimhalu does not describe configuring the computer itself, let alone configuring the computer to operate in a <u>full-access mode</u> in which the computer permits <u>both read and write access</u> to the storage device. In fact, Narasimhalu is entirely devoid of any discussion regarding controlling both read and write access to the storage device itself, and makes no mention of configuring a computer to permit both read and write access to the storage device based on device-specific security information stored on that device. Applicants have amended claim 1 to clarify that, in one claimed embodiment, the computer permits both read and write access to the storage device itself in the full-access mode.

With respect to the requirement of operating in a restricted-access mode, the Examiner asserted that Narasimhalu discloses halting installation when incorrect non-uniformities are detected on the distribution medium. In particular, the Examiner states that "'to halt the program altogether' is read as 'operating the storage device in a read-only mode.'"[2] This interpretation is clearly inconsistent with the teachings of Narasimhalu. In particular, Narasimhalu makes clear that the distributed information is <u>read</u> and installed from the distribution medium only if correct media non-uniformities are detected.[3] Otherwise, installation is halted entirely, i.e., information

[1] *Abstract; col. 4, ll. 12-25.*
[2] *Office Action, page 7.*
[3] *See FIGS. 7A, 7B and related disclosure.*

is not read from the distribution medium. Again, Applicants have amended claim 1 to clarify that in the full-access mode the computer permits both read and write access to the storage device, and that in the restricted-access mode the computer permits read access to the storage device and prevents write access to the storage device.

With respect to claim 2, as another example, Narasimhalu fails to teach or suggest encrypting digital data to be written to the storage device from the computer, and decrypting digital data read from the storage device by the computer. Narasimhalu describes a process in which an "information provider" utilizes the copy protection scheme to prepare a distribution package by storing encrypted information on the distribution medium. Subsequently, a consumer is able to install or read the encrypted information only when correct non-uniformities are detected within the distribution medium. Consequently, Narasimhalu does not describe configuring a computer to operate in a full-access mode in which the computer permits both read and write access to the storage device, and automatically encrypts and decrypts a data stream associated with the read and write access to the storage device.

To further illustrate the deficiencies of Narasimhalu, Applicants refer the Examiner to claim 51. With respect to claim 51, Narasimhalu fails to teach or suggest a computer comprising a drive for accessing a data storage device having device-specific security information stored thereon, and a storage manager to selectively configure the drive to operate in a full-access mode of operation or a restricted-access mode of operation as a function of the device-specific security information stored on the storage device. Applicants have amended claim 51 to clarify that, in this claimed embodiment, the drive permits both read and write access to the storage device in the full-access mode, and permits read access to the storage device and prevents write access to the storage device in the restricted-access mode.

In contrast with these requirements, Narasimhalu merely discloses a copy protection scheme in which installation (or read access) of encrypted information is either permitted or aborted based upon detecting correct or incorrect medium non-uniformities. Narasimhalu does not describe configuring a drive at all, let alone configuring the drive to operate in either a full-access mode or a restricted access mode based on device-specific security information stored on a storage device.

Claim 61, 63-66 and 67

In addition, the Examiner rejected claims 61, 63-66 and 67 under 35 U.S.C. 102(b) as being anticipated by Michael Angelo (US 5,887,131). Applicants respectfully traverse the rejection to the extent such rejection may be considered applicable to the amended claims. Angelo fails to disclose each and every feature of the claimed invention, as required by 35 U.S.C. 102(b), and provides no teaching that would have suggested the desirability of modification to include such features.

With respect to claim 61, for example, Angelo fails to disclose a first storage device having format information stored thereon, a second storage device having data stored thereon, and a software module executing within the computing system, wherein the software module selectively permits access to the data of the second storage device as a function of the format information stored on the first storage device.

In rejecting claim 61, the Examiner states that Angelo discloses that a smart card is used to store an authorization value needed to enable power to a computer system or access to secured resources. The Examiner then states that "this reads on 'format information and security information stored on the first storage device.'" Applicants respectfully disagree with this assertion. The Examiner is apparently either entirely disregarding the term "format information" as required by Applicants' claim 61, or is interpreting the term in a manner entirely inconsistent with its use within the present application, which is impermissible.

For example, the present application clearly describes format information as generated during the process of formatting the storage medium (see, e.g., description of FIG. 3A). The present application describes the format information as inherently unique to the storage device, and provides examples of format information, such as lists of bad sectors. The Examiner's conclusion that the claim element "format information" reads on an "authorization value" is clearly incorrect. Applicants respectfully remind the Examiner that terms within a claim must be interpreted in light of the other claims and the specification in order to ascertain their intended meaning.[4] It is impermissible to construe terms within Applicants' claims in a manner that is entirely inconsistent with their plain meaning and the specification of the present application.

[4] *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 979 (Fed. Cir. 1995) (in banc), *aff'd*, 116 S. Ct. 1384 (1996).

With respect to claim 65, it again appears the Examiner has either disregarded or overlooked certain elements of Applicants' claim. For example, claim 65 requires a software application that generates a cryptographic key as a function of the format information of the first storage device and format information of the second storage device. In other words, a cryptographic key is generated from format information from two different storage devices. In rejecting this claim, the Examiner merely referred to the smart card of Angelo and its stored authorization value. As described above, Angelo makes no mention of utilizing format information of a first storage device to control access to a second storage device at all, let alone using a cryptographic key generated from format information from two different storage devices.

The cited references fails to disclose each and every limitation set forth in claims 1-6, 12, 18, 20-21, 26-33, 45-49, 51-54, 56-61 and 63-67. For at least these reasons, the Examiner has failed to establish a prima facie case for anticipation of Applicants' claims under 35 U.S.C. 102(b). Withdrawal of this rejection is requested.

Claim Rejections Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 7, 34-36 and 44 under 35 U.S.C. 103(a) as being unpatentable over Narasimhalu in view of Moore (US 6,067,622). In addition, the Examiner rejected claims 9-11 and 62 under 35 U.S.C. 103(a) as unpatentable over Narasimhalu et al (US 5,412,718) in view of Watson et al. (US 5,475,839). The Examiner also rejected claims 22-25, 50 and 55 under 35 U.S.C. 103(a) as unpatentable over Narasimhalu et al (US 5,412,718) in view of Epstein (US Patent Application Number 2002-0124176A1).

Applicants respectfully traverse these rejections. The applied references fail to disclose or suggest the inventions defined by Applicants' claims, and provide no teaching that would have suggested the desirability of modification to arrive at the claimed invention. These claims include the limitation of the base claims on which they depend, and are patentable for at least the reasons set forth above with respect to these claims. Moreover, the cited references do not overcome the deficiencies of Narasimhalu described above.

In addition, with respect to claim 9, the cited references fail to teach or suggest sensing whether a storage device has device-specific security information stored thereon, and operating a computer in a full-access mode including permitting a user to access sensitive data stored on a remote computer when the storage device has the device-specific security information. With respect to these requirements, the Examiner asserts that it would have been obvious to modify the copy protection scheme of Narasimhalu to extend to remote computers in view of Watson, which describes a method by which a supervisor can control security information stored locally on an individual's computer.

The Examiner's conclusion of obviousness is incorrect for many reasons. Neither Narasimhalu, Watson, nor any other cited reference teaches or suggests sensing whether a storage device has security information that is specific to that storage device (e.g., low-level format information), and operating a computer in a full-access mode to permit a user to access sensitive data stored not on that storage device but on a remote computer. Thus, even modification of the copy protection scheme of Narasimhalu in view of Watson would not achieve Applicants' invention as claimed.

Moreover, Narasimhalu describes a copy protection scheme for distribution of software or other information to consumers, e.g., the sale of software. In other words, Narasimhalu is entirely focused on protection of the distributed software (or other information) contained on the distribution medium (e.g., diskette). The Examiner states that the modification of Narisimhalu scheme would allow information to be shared among multiple computers. To the contrary, at best, modification of the copy protection scheme Narasimhalu as suggested by the Examiner would possibly allow distributed information to be installed on multiple computers. It certainly would not achieve Applicants' claimed invention of sensing device-specific information, and operating a computer to permit a user to access sensitive data stored on a remote computer.

In similar manner, neither Narasimhalu or Watson or any other reference teaches or suggests sensing whether a storage device has device-specific security information stored thereon, operating the computer in full-access mode including permitting the user to access a second storage device when the storage device has the device-specific security information, as required by claim 10.

With respect to 20, the cited references fail to teach or suggest detecting a storage device within a storage drive, sensing whether the storage device has security information generated from a combination of device-specific information associated with the storage device and user-specific information associated with a user, configuring the storage drive to prevent write access to the storage device when the security information is not sensed, and configuring the storage drive to permit write access by encrypting digital data using the security information and writing the encrypted digital data to the storage device when the security information is sensed.

With respect to these claim elements, the Examiner asserts that it would have been obvious to one of ordinary skill in the art to modify the copy protection scheme of Narasimhalu in view of an access security system described by Epstein that utilizes user (e.g., biometric information). However, Epstein fails to overcome the deficiencies of Narasimhalu discussed above. Consequently, even if Narasimhalu were modified in view of Epstein, Applicants' claimed invention would not be achieved. For example, neither Narasimhalu nor Epstein teaches or suggests configuring a storage drive to prevent write access to the storage device when the security information is not sensed, and configuring the storage drive to permit write access by encrypting digital data using the security information and writing the encrypted digital data to the storage device when the security information is sensed, as required by claim 20, as amended.

Moreover, as described above, Narasimhalu discloses a copy protection scheme for preventing unauthorized copying of distributed software. According to Narasimhalu, an "information provider" utilizes the copy protection scheme to prepare a distribution package by storing encrypted information on the distribution medium. Subsequently, e.g., after purchasing the software, a consumer is able to install or read the encrypted information only when correct non-uniformities are detected within the distribution medium. Typically, the individual consumers of the distribution packages would not be known at the time of manufacturing when the packages are prepared for distribution. Consequently, it is speculative at best to suggest that user-specific information, such as biometric information, could be utilized with the distribution scheme described by Narasimhalu. Neither Narasimhalu nor Epstein teaches or suggests a manner in which the modification suggested by the Examiner could be achieved.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicants' claims 7, 9-11, 22-25, 34-36, 44, 50, 55 and 62, under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

CONCLUSION

All claims in this application are in condition for allowance. Applicants respectfully request reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 09-0069. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date:

2/16/4

Imation Legal Affairs
P.O. Box 64898
St. Paul, Minnesota 55164-0898
Telephone: (651) 704-3604
Facsimile: (651) 704-5951

By:

Eric Levinson

Name: Eric D. Levinson
Reg. No.: 35,814